ARAMOHO HEALTH CENTRE
Privacy Policy and Procedure

---

1. PURPOSE

To outline how the personal health information of individuals, held by Aramoho Health Centre (AHC), will be managed, protected and respected.

2. SCOPE

This policy applies to all general practitioners, employees, contractors, locums, trainees and students working in or for AHC.

3. RESPONSIBILITIES

- Under the Privacy Act 2020, agencies must follow a set of rules when handling personal information.
- The Health Information Privacy Code 2020 sets specific rules for agencies handling health information.
- Section 201 of the Privacy Act 2020 requires agencies to appoint a Privacy Officer who is responsible for:
  - Ensuring the agency complies with the Act
  - Dealing with any complaints from the organisation's clients about possible privacy breaches
  - Dealing with requests made to the agency for access to, or correction of, personal information
  - Working with the Privacy Commissioner's Office when it investigates complaints
  - Encouraging the agency to comply with the Information Privacy Principles
- AHC will ensure all staff undertake training on the Privacy Act 2020 and the Health Information Privacy Code as part of their orientation programme, and that they complete training updates when deemed necessary by the Privacy Officer.
- While AHC has a responsibility to ensure that it takes reasonable steps to ensure employees adhere to the Act, in some cases, the individual staff member may be held directly liable. All employees, contractors, locums, trainees and or students working in or for AHC will sign a confidentiality agreement prior to commencing work for AHC (Appendix Two).

4. POLICY AND PROCEDURE

The framework for the collection, exchange and management of health information about identifiable individuals falls within the provisions of the Privacy Act 2020 (the Act) and the Health Information Privacy Code 2020 (HIPC).

The **Privacy Act 2020** controls how agencies collect, use, disclose, store and give access to 'personal information'.

The **Health Information Privacy Code 2020** sets specific rules for agencies in the health sector. It covers health information collected, used, held and disclosed by health agencies and takes the place of the information privacy principles for the health sector.

The Code applies to personal information about an 'identifiable individual', including:

- medical and treatment history
- disabilities and accidents
- recordings and photographs
- contact with any health / disability provider
- information about donations of organs, blood, etc.
- incidental information obtained while providing services such as billing, subsidy entitlements, etc.

4.1 Collection of health information

Any information collected by AHC will be related to:

- the patient's care and treatment
- administrative purposes such as billing and claims management
- monitoring quality of patient care, treatment and health status such as audit.

Information will be collected from the individual concerned in the first instance except where:

- the patient has authorised collection from someone else
- the collection of information from the patient is not reasonably practical
- the collection of information from the patient would prejudice their interests, the purpose of collection, or the safety of any person.

When collecting information, staff will either inform patients verbally by way of explanation or by including written advice in documents sent to new patients e.g. enrolment forms:

- that the information is being collected
- why the information is being collected
- who will receive the information
- whether the provision of the information is voluntary or involuntary
- any consequences if the information is not provided
- access and correction rights in relation to the information

AHC will:

- only collect information that is necessary
- be sensitive about who collects the information and how it is collected
- determine who has access to it
- ensure conversations either cannot be overheard when collecting information verbally (in person, or over the telephone).

Where information is collected from someone other than the patient, AHC staff will ensure that this is noted on the patient record. When, or if, appropriate, the accuracy should be checked with the patient in order to ensure compliance with rules 7 and 8.

4.2 Retention of health information

In accordance with the Health (Retention of Health Information) Regulations 1996, patient notes may be destroyed after ten years following their last contact with the health facility.

The minimum retention period of 10 years begins from the day after the date shown in the health information as the most recent date on which a provider provided services to that individual.

4.3 Destruction of material containing identifiable health information

All material containing identifiable health information that is not required to be kept as part of an individual's medical record (e.g. copy of scanned document) must be placed in the secure destruction bin.

4.4 Access to and disclosure of health information

Access and disclosure of health information will be in accordance with the AHC Access and Disclosure of Patient Information Policy and Procedure.

4.5 Correction of health information

Where AHC holds health information, the individual patient concerned has the right to request correction of the information and AHC must help facilitate access and correction requests when they are made. In the situation where AHC is not willing to amend the information in accordance with such a request, AHC must append to the health information:

- advice noting the individual has questioned the accuracy of the information
- any statement provided by the individual in regard to the correction sought, so it will be read with the information

AHC will advise the requester that they have the right to complain to the Privacy Commissioner and to seek an investigation and review of a decision to not amend health information.

4.6 Security of information

Access to AHC premises will be in accordance with the AHC Building Security Policy. Server rooms, filing cabinets, storage areas and unattended rooms will be locked when not in use and access restricted to authorised personnel. Off-site storage used for storing records will be secure and records retrievable. When a staff member leaves all keys must be returned and computer access disabled.

All information displaying or containing patient information will be kept securely, away from or out of view of unauthorised people:

- Verbal information relating to an identified patient's health history and/or results will be not be relayed in public areas.
- Written documentation should be placed face down on desktops.
- Staff must ensure that any information displayed on PMS screens is not visible to the public or in consulting rooms, relates to the patient who is present.
- AHC email and facsimile header sheets will contain a privacy caution.
- Identifiable information no longer required by the practice will be destroyed or deleted in a secure manner.

- Access to reception areas is restricted. When temporarily unstaffed, entrance doors must be kept locked preventing public access.

4.7 Confidentiality

All staff members must understand and sign a confidentiality agreement as part of their employment agreement or contract of service. The obligations under this agreement extend after the employment or contract arrangement has ended.

4.8 IT systems

IT security and confidentiality will be set and maintained in accordance with AHC policy. Passwords, automatic log off after periods of inactivity and use of screen savers are compulsory.

All AHC employees are discouraged from making data portable through USB, CDs, or portable media. The Privacy Officer must be consulted before any information identifying staff or patients is copied to portable media.

4.9 Telehealth

The New Zealand Medical Council expects that the treatment provided to a patient in another location meets the same standards as care provided in an in-person consultation. This includes maintaining the patient's privacy and confidentiality.

The transfer of patient information during telehealth consultations should be private and confidential and AHC will facilitate this through the following procedures:

- Telehealth consultations should only take place in areas where privacy and confidentiality can be maintained (e.g. consultation rooms with the door closed).
- Telehealth consultations conducted remotely (e.g. from a health practitioner's home) must maintain the same privacy and confidentiality standards as practiced within the health centre buildings.
- Any device, software or service used for the purpose of telehealth must be secure and fit for purpose.
- Patients participating in the telehealth consultation should be asked to confirm their identity and identify where they are at the time of the consultation. Patients should be advised to move to a quiet, private space if necessary. The consent of the patient is implied by them initiating or accepting the consultation, however good practice is to confirm this on commencing.
- AHC staff should not enter a space where a telehealth consultation is taking place without taking privacy and confidentiality precautions (e.g. knocking on door and waiting for answer before entering a room, not disturbing clinical staff participating in telehealth consultations)
- If any part of a telehealth consultation is to be recorded, this record must be stored securely so that privacy and confidentiality of health information is maintained.
- If there is a valid and clinically appropriate reason for the recording of a consultation, patients must be fully informed and give consent.
- Appropriate storage of any reports provided for, or generated from, the telehealth consultation must be maintained.

- Video consultations should be conducted via the patient portal ManageMyHealth™.

4.10 Patient Portal

AHC, through Whanganui Regional Health Network, has a contract to use the ManageMyHealth™ patient portal. ManageMyHealth™ is hosted in a secure environment in New Zealand, and uses Transport Layer Security (TLS 1.2), a cryptographic protocol used to establish a secure communications channel between two systems. It is used to authenticate one or both systems, and protect the confidentiality and integrity of information that passes between systems.

Use of the patient portal to provide access to consultation notes must be agreed with each individual patient. Patients register for a portal by providing an email address and proof of identity so they can be sent a login and password. AHC will contact patients directly to verify identity of online registrations. The practice will provide an activation code and instructions on how to complete registration online. Risk is lowered where complex passwords are required to gain access. The biggest risk is if a patient gives someone else their username/password. An audit trail can show who has accessed the portal to give patients certainty that their information has been seen only by authorised staff. Staff access to ManageMyHealth™ is through secured PMS login.

4.11 Privacy Officer

The practice Privacy Officer is the Practice Manager. They have received training and are aware of their responsibilities. The Privacy Officer has overall responsibility for privacy issues in the practice, but all staff are responsible for ensuring they keep up to date with their obligations under this legislation

Privacy Officer role:

- Ensure that the practice has a current privacy policy and procedures and that all staff can easily access these documents.
- Ensure that all staff members have read and understood the policy and procedures, and this has been documented.
- Ensure that the practice complies with the Privacy Act, both in regard to personal patient information and employee information.
- Deal with requests made to the practice about personal or employment information.
- Ensure compliance with the Health Information Privacy Code in relation to patient information.
- Brief the practice team on changes to legislation and/or practice processes.
- Use team meetings to discuss privacy complaints received, the part of the procedure that failed and ways to improve the process.
- Continuous improvement process and education.
- Induction of new staff on Privacy and HIPC.
- Source suitable training opportunities.
- Ensure that any complaints received are dealt with in accordance with legislation. If referred to Privacy Commission work with them to resolve.
- Provide clear guidelines to staff around who has access to health information and how it is handled.

4.12 Privacy Breaches

A privacy breach is where there has been unauthorised or accidental access to personal information, or disclosure, alteration, loss or destruction of personal information. It can also include a situation where a business or organisation is stopped from accessing information – either on a temporary or permanent basis.

If AHC has a privacy breach which has caused serious harm to someone (or is likely to do so), the Privacy Officer must be informed as soon as possible.

Examples of likelihood of serious harm being caused by a breach include:

- Physical harm or intimidation
- Financial fraud including unauthorised credit card transactions or credit fraud
- Family violence
- Psychological, or emotional harm

If a notifiable privacy breach has occurred, the Privacy Officer will notify the Office of the Privacy Commissioner and affected individuals as soon as possible.

- The Office of the Privacy Commissioner has an online tool 'notify us' to evaluate whether privacy breaches are notifiable, and report them.

4.10 Complaints of Breach of Code

The AHC Privacy Officer will deal with any complaints alleging a breach of the HIPC and facilitate the fair, simple, speedy, and efficient resolution of complaints through compliance with the following process:

(i) Acknowledge the complaint in writing within 5 working days of receipt, unless it has been resolved to the satisfaction of the complainant within that period; and
(ii) Inform the complainant of any relevant internal and external complaints procedures; and
(iii) Document the complaint and the actions of AHC.

Within 10 working days of acknowledging the complaint, AHC must decide whether it:

(iv) Accepts that the complaint is justified; or
(v) Does not accept that the complaint is justified; or
(vi) Decides that more time is needed to investigate the complaint.

If that additional time is more than 20 working days, AHC must:

(vii) Inform the complainant of that determination and of the reasons for it.

As soon as practicable after deciding whether or not it accepts that a complaint is justified, AHC must inform the complainant of:

(viii) The reasons for the decision; and
(ix) Any actions it proposes to take; and
(x) Any appeal procedure the agency has in place; and
(xi) The right to complain to the Privacy Commissioner.

5. DEFINITIONS

AHC: Aramoho Health Centre Ltd
HIPC: Health Information Privacy Code
OPC: Office of the Privacy Commissioner

6. MEASUREMENT CRITERIA

- Evidence of training completion
- Number of breaches and actions taken recorded in Incident Register

7. REFERENCES

HISO 10064:2017 Health Information Governance Guidelines
Office of the Privacy Commissioner
New Zealand Medical Council Statement: Telehealth. March 2020
HISO 10029:2015 Health Information Security Framework

8. RELEVANT LEGISLATION

Code of Health and Disability Consumer's Rights 1996.
Human Rights Act 1993
Health and Disability Commissioner Act 1994
Health Information Privacy Code 2020
NZ Bill of Rights Act 1990
Privacy Act 2020

9. ASSOCIATED DOCUMENTS

Consumer Rights Policy
Access and Disclosure of Patient Information Policy and Procedure
Patient Information Management Policy
Building Security Policy
Patient Enrolment Policy and Procedure
Clinical Records Policy

10. APPENDICES

Appendix One: Health Information Privacy Code Summary
Appendix Two: AHC Confidentiality Agreement
Appendix Three: Privacy Access Escalation Ladder

Any breach of AHC policy by employees will be treated as a Human Resources issue. Serious breaches will be dealt with immediately.

APPENDIX ONE

Summary - Rules of the Health Information Privacy Code

The Health Information Privacy Code has thirteen rules:

- Rules 1, 2, 3 and 4 govern the collection of health information. This includes the reasons why health information may be collected, where it may be collected from and how it is collected.
- Rule 5 governs the way health information is stored. It is designed to protect health information from unauthorised use or disclosure.
- Rule 6 gives individuals the right to access their health information.
- Rule 7 gives individuals the right to correct their health information.
- Rules 8, 9, 10 and 11 place restrictions on how people and organisations can use or disclose health information. These include ensuring information is accurate and up-to-date and is not improperly disclosed.
- Rule 12 governs the disclosure of health information outside of New Zealand.
- Rule 13 governs how 'unique identifiers' - such as Inland Revenue Department (IRD) numbers, bank client numbers, driver's licence and passport numbers - can be used.

APPENDIX TWO

CONFIDENTIALITY AGREEMENT

I……recognise that in my position

as…….. At Aramoho Health Centre Ltd

I will be exposed to patients' health information.

I understand the need to keep patients' health information confidential and secure at all times.

I understand that this obligation continues even after I cease working at the practice.

I also understand that I must keep confidential any private knowledge that I gain about staff in the course of my employment.

Signed……..

Date……

APPENDIX THREE

Privacy access escalation ladder

The escalation ladder

Sharing information involves both the collection and disclosure of personal information. Deciding which laws apply and what information to share can be complicated, but there are some guiding rules.

How to use the escalation ladder

Work through from question 1 to question 5 and stop when you can answer 'yes'.

If the answer to all of the five questions is 'no', then disclosure should be unnecessary and should be avoided, at least for now.

Remember that the proportionality principle always applies – you should only provide as much information as is reasonably necessary to achieve your objectives.

Question 1: Can we get by without naming names?

- Use anonymous information where practical.
- Disclosing anonymous information is always okay.

Question 2: Have they agreed?

- If information is not able to be used anonymously, the best thing is consent from the parties concerned.
- Consent does not need to be written.
- Always record the fact that parties have agreed. Record any limitation or qualification of consent, eg, "please don't involve the church".

Question 3: Have we told them?

- If it is not practicable or desirable to obtain consent, the information may be used or disclosed if it is in line with the purpose for which it was obtained.
- Inform the person affected of this where possible – ideally at the time the information was first collected from them, or soon after that.
- If informing the person would prejudice the purpose of collection, or would be dangerous to any person, then telling the person concerned may be waived in that instance.

Question 4: Is there a serious threat

Information may be used or disclosed where there is a serious threat.

What is considered serious depends on:

- how soon the threatened event might take place
- how likely it is to occur
- how bad the consequences of the threat eventuating would be.

Question 5: Is there another legal provision we can use?

Many different laws allow personal information to be shared. For instance, health information:

- about the health/safety of a child or young person can always be disclosed to a police officer or social worker
- can be requested by someone who needs it to provide health services
- can be disclosed where necessary to avoid prejudice to the maintenance of the law
- can be shared under an AISA.

If the answer to all of the five questions is 'no', then disclosure should be unnecessary, and should be avoided, at least for now.